



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,697	04/18/2006	Marian Trinkel	20811/0204765-US0	1949
7278	7590	03/09/2010	EXAMINER	
DARBY & DARBY P.C. P.O. BOX 770 Church Street Station New York, NY 10008-0770			ARMOUCHE, HADIS	
			ART UNIT	PAPER NUMBER
			2432	
			MAIL DATE	DELIVERY MODE
			03/09/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/541,697	Applicant(s) TRINKEL, MARIAN
	Examiner HADI ARMOUCHE	Art Unit 2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 19 November 2009.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 04/18/2006 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/GS-68)
 Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 11/19/2009. Claims 1-3, 9 and 18-19 have been amended. Claims 1-20 remain pending.

Response to Arguments

2. Applicant's arguments filed on 11/19/2009 have been fully considered but they are not persuasive.

3. It has been argued (page 8 of the remarks) that Fruehauf does not teach or suggest synchronously creating a key at the user and central system and that Sinha does not teach or suggest synchronously creating a key by respective clock system.

4. Applicant's interpretation of the references is noted. However examiner respectfully disagrees. The rejection was structured so that the three references (Hartman, Fruehauf and Sinha) would be taken in combination. Hartman teaches encrypting the time signal using a key at the central system before sending it to the network user. However, Hartman does not explicitly teach that the encryption key used at the central system is the same as the decryption key used by the network user (symmetric key). Fruehauf teaches synchronizing the keys such that the receiving and the sending side share identical keys (col 4 lines 62-64). Moreover, applicant admits in paragraph 0010 of the specification that it is well known in the art to use one key for encryption and decryption of the time signal. Therefore, it would have been obvious to modify Hartman's method with Fruehauf's teachings to manage the keys easier and to increase the speed of the system since symmetric-key algorithms are generally much less computationally intensive than asymmetric key algorithms. Sinha teaches a system

in which plurality of clock pairs, in the form of master and slave clocks, are commonly used across a network. It would have been obvious to modify the combined system of Hartman and Fruehauf with Sinha's teachings to synchronize the key generated/created.

5. Examiner invites the applicant to schedule an interview with the examiner prior to the next communication.

Specification

6. The disclosure is objected to because of the following informalities: Figure 1 shows that the connection 14 is connected with network user 1e whereas paragraph 0039 of the specification teaches that it is network user 1c. Appropriate correction is required.

Claim Objections

7. Claims 19 and 20 are objected to because of the following informalities: Claims 19 and 20 are method claims that depend on system claim 9. For the purpose of examination, examiner assumed that the applicant meant to say "the system as recited in claim 9....". Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-3, 9-11, 15-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman Jr. (5,444,780), hereafter referred to as Hartman, in view of

Fruehauf et al. (US 6,590,981), hereafter referred to as Fruehauf, and further in view of Sinha et al. (US 6,944,188), hereafter referred to as Sinha.

Regarding claim 1: A system in which a central system receives a time signal request, encrypts the time signal using a key, transmits the encrypted time signal to the requesting user, and provides the network user with the same key can be seen in **Hartman column 4, lines 54-56, 66-68; column 5, lines 28-43**, which discloses a client computer requesting a time signal from a recognized server. The server responds to the request by sending an encrypted time signal to the client. The client then decrypts the time signal using the same key that the server used to encrypt it.

Hartman fails to explicitly disclose synchronously creating a key using a respective clock system of the central system and of the network user uniquely assigned to the network user.

However, **Fruehauf column 2, lines 14-34; column 4, lines 22-64** discloses a system that creates keys synchronously at two different locations.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously create symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Hartman and Fruehauf fail to disclose a clock system in which clocks at both the central system and the network user are uniquely assigned to each other.

However, **Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64**

discloses a system in which a plurality of clock pairs, in the form of master and slave clocks, are commonly used across a network.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Regarding claims 2 and 19: A system that dynamically changes symmetric keys after a predetermined period of time can be seen in **Fruehauf column 2, lines 7-10, 14-34**, which discloses a cryptographic communication system with time synchronized keys that change after a predetermined period of time, being used for encryption and decryption between sender and receiver locations.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to dynamically change symmetric keys, as taught in Fruehauf, as changing keys creates an extremely high entry barrier for hackers, and changing keys synchronously at two different communication points.

Regarding claims 3 and 11: Hartman fails to explicitly disclose a system that synchronously creates keys using a respective clock system of the central system and of the network user uniquely assigned to the network user.

A system that synchronously creates keys at two different locations can be seen in **Fruehauf column 2, lines 14-34; column 4, lines 22-64.**

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously create symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Hartman and Fruehauf fail to disclose a clock system in which clocks at both the central system and the network user are uniquely assigned to each other.

However, **Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64** discloses a system in which a plurality of clock pairs, in the form of master and slave clocks, are commonly used across a network.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Regarding claim 9: A central system with a network user, wherein the central system encrypts a time signal, sends the time signal to the user, and the user decrypts the key can be seen in **Hartman column 4, lines 54-56; column 5, lines 28-43**, which discloses a system with a server coupled to a client. The server encrypts the time information and sends it to the client for decryption.

However, Fruehauf column 2, lines 14-34; column 4, lines 22-64

discloses a system that creates keys synchronously at two different locations.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously create symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Hartman and Fruehauf fail to disclose a clock system in which clocks at both the central system and the network user are uniquely assigned to each other.

However, Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64
discloses a system in which a plurality of clock pairs, in the form of master and slave clocks, are commonly used across a network.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Regarding claim 10: A system in which the central system includes a time signal transmitter can be seen in **Sinha column 3, lines 5-11; column 7, line 61 to column 8, line 3; Fig. 3**, which discloses a system that uses a transmitter as part of the master clock.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to include a signal transmitter, as taught by Sinha, in order to allow for a communications over a wider area.

Regarding claim 15: A system in which a user decrypts an encrypted time signal can be seen in **Hartman column 5, lines 38-43**, which discloses a system where the client decrypts the encrypted time signal that it received from a secure time server.

Regarding claims 16, 17, and 20: A system in which the central system is a certified central system can be seen in **Fruehauf column 3, line 47 to column 4, line 15**, which discloses a system that uses officially recognized time sources to create a time signal.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time sources, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf, and Sinha, and in further in view of Crane et al. (US 6,510,236), hereafter referred to as Crane.

Regarding claim 4: A system where the central server receives a time-signal request from the network user can be seen in **Hartman column 4, lines 54-56, 66-68; column 5, lines 28-43**, which discloses a client computer requesting a time signal from a recognized server.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time sources, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

However, Hartman, Fruehauf, and Sinha fail to explicitly disclose a system that determines, by the central system, a clock system assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user.

However, **Crane column 4, line 48 to column 5, line 36** discloses a system in which a device-id is used to locate the corresponding server.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use a device's corresponding id, as taught by Crane, as the device's id is known by both parties and can easily be used to create corresponding symmetric keys.

11. Claims 5-8 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf and Sinha, and further in view of Kara (US 5,982,506), hereafter referred to as Kara.

Regarding claim 5: Hartman and Fruehauf fail to explicitly disclose a system that transmits the time signal and the data from the first network user to the second network user using one of directly and indirectly via the central system.

However, **Kara column 19, lines 19-31** discloses a system in which a sender and a receiver communicate directly with one another without the intervention of a central system.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the sender and receiver to communicate with each other without relying on a central system, as taught in Kara, to hasten transaction speed between the two devices.

Kara column 4, lines 25-56 discloses an invention that sends a message from a sender to a receiver via a certification system.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to send a message indirectly through a central system, as taught by Kara, so that the send time may be verified and certified by an external third party.

Regarding claim 6: A system in which the first network user encrypts at least one of the data and the time signal during transmission can be seen in **Kara column 4, lines 43-48; column 7, lines 43-45**, in which the electronic document and/or the cipher containing the timestamp may be encrypted.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to encrypt the electronic document containing the timestamp, as taught by Kara, to prevent potentially erroneous or malicious data from entering into a secure system.

Regarding claim 7: A system in which the central system can be provided at the second network user can be seen in **Kara column 25, lines 47-61**, in which the certification and key distribution authority can be located at the receiving location.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the central system to be located at the second network user, as taught by Kara, in order to hasten the key generation process and ensure symmetric key coordination.

Regarding claim 8: A system in which the central system returns an acknowledgment to the network user can be seen in **Kara column 4, line 65 to column 5, line 22**, in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement

message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

Regarding claim 12: A system in which the central system can be provided at the second network user can be seen in **Kara column 25, lines 47-61**, in which the certification and key distribution authority can be located at the receiving location.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the central system to be located at the second network user, as taught by Kara, in order to hasten the key generation process and ensure symmetric key coordination.

Regarding claim 13: A system in which the central system returns an acknowledgement to the network user can be seen in **Kara column 4, line 65 to column 5, line 22**, in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

Regarding claim 14: A system in which the central system returns an acknowledgment to the network user can be seen in **Kara column 4, line 65 to column 5, line 22**, in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf, Sinha and Crane, and further in view of Friedman et al. (US 2002/0019933), hereafter referred to as Friedman.

Regarding claim 18: Hartman, Fruehauf, Sinha, and Crane fail to explicitly disclose that the key is created using at least one of the assigned clock and the transmitted identifier.

However, **Friedman [0101]** discloses a system in which a key is derived using information unique to the particular requesting device.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use a device's corresponding id, as taught by Friedman, as the device's id is known by both parties and can easily be used to create corresponding symmetric keys.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432